Remarks

I. Status of Claims

Claims 1-6 and 8-21 are pending in the application and stand rejected.

Claims 1, 4, 5, and 6 are in independent form.

The current Office action rejected claims 1-15 under 35 U.S.C. § 102(e) as allegedly being anticipated by U.S. Patent No. 6,714,944 ("Shapiro") (Office action, page 3). However, it appears that claims 16-21 also were rejected over Shapiro. (See Office action, page 8.) Applicant respectfully traverses these rejections and requests reconsideration.

In this reply, claims 1, 5 and 6 are amended. Claim 2 is canceled. No new claims are added. Thus the pending claims are 1, 3-6 and 8-21.

II. Brief Summary of Shapiro

1. Shapiro leaves control of verification up to the user-subject.

The system disclosed by Shapiro is exposed to fraud and abuse because the user [subject] selects what data to enter into the system, and what third parties to contact for verification of that data.[1] "Once the registrant has entered data through process 21, the data is used for verification process 22."[2] The user may have conspired with those third parties, for example a prior employer, to provide affirmative responses to verification inquiries. It would be important to instead determine whether information supplied by a user is valid based on external (third-party validator) data that is not under the user's control.

More specifically, Shapiro provides for a user ("Registrant") to select and enter whatever data the user chooses; see the "Registrant data-entry process" 21 in FIG. 2.[3] The system of Shapiro subsequently undertakes to verify the data input and stored by the user (22), by contacting third parties which, again, are specified by the user.[4]

---

[1] See Shapiro FIGS. 4A and 4B (registrant data-entry process), and text at 7:18-8:40. (References herein are to patent [*column number*][:][*line numbers*].)

[2] Shapiro 6:3-4.

[3] See Column 7, lines 18-55.

[4] See Column 7, line 56 to Column 8, line 36.

2. Key Distinctions Between "In-Wallet" and "Out-of-Wallet" Data

"In-wallet" data is information you know about yourself or can readily put your hand to. It includes, for example, your name, address, telephone number, drivers license number, social security number, checking account number, credit card numbers, mother's maiden name, and the like. You know all this or can readily get it, say by looking in your purse or wallet.[5] (This data forms the basis for some of the simpler authentication systems of the prior art.)

"Out-of-wallet" data is information about you that would take you a little effort to find out, but that you probably have in your home filing system or somewhere equally accessible with some effort. It includes, for example, information such as the amount of the last transaction with your checkbook or credit card, the holder and amount of your mortgage, your credit rating, your bank balance, and the like. Incorporating out-of-wallet information into an authentication system admittedly is more complicated, but it provides greater reliability.[6] Claim 1 is currently amended to call for requiring the subject to provide out-of-wallet data in response to a query generated by the verification engine.

3. Understanding the "Players" and their Roles

The verification engine in a preferred embodiment accepts personal data from a *subject* being authenticated. (The *subject being authenticated* is analogized by the examiner to the "user" described in Shapiro.)[7] As used throughout these systems and the attached claims, the entity requesting authentication of the subject is termed the "authentication client" or "client." See the E-Commerce Site (15) in FIG. 2 as one example. In use, the *subject* may be a potential customer (1) logged into the E-Commerce Site (15). The E-Commerce Site (vendor) uses the Authentex *verification engine* (10) to

[5] See specification, paragraph [0005].

[6] See specification, paragraph [0006].

[7] Typically, the data useful for authentication of the subject's identity can be collected from the subject as part of a financial transaction with an agency of the federal government, financial institution, or commerce entity, or incident to some security procedure, etc. For example, when one goes to a financial institution to secure a loan, that institutution not only collects "out-of-wallet" data but it also physically verifies that data. See applicant's **FIG. 2** – where the lender is an example of a "trusted validator" (3a), and it conducts "physical validation" (2), of data provided by the customer (1). Here, the "customer" is the *subject* whose identity is to be validated.

verify the identity of the customer as further discussed below, using cooperation of one or more independent trusted validators (3a,3b).

4. Shapiro attempts to verify only information selected and provided by the user.

By contrast, we present out-of-wallet queries to the user[8] who seeks to authenticate his identity, and he has no prior knowledge of what those questions might be. Further, neither the verification engine nor the *authentication client* generally know the answer – rather, the user's (*subject's*) response is submitted to a cooperating third-party database proprietor ("trusted validator" 3 in Figure 2). That validator then responds to the verification engine with a confidence level as to whether the user's response (requesting "out-of-wallet" data) matches a record in the third-party database. In this way, the user-supplied response is verified against independent third-party data, not against data previously submitted and stored by the user himself.

III. Specific Discussion of Claim 1

Claim 1 as currently amended recites:

1. (Currently amended) A user identity authentication system comprising:

an authentication client for requesting authentication of a subject;

a client interface to receive the authentication request from the authentication client;

multiple independently operated databases, each database storing ~~information~~ out-of-wallet data associated with the subject, the associated ~~information~~ out-of-wallet data being accessible only through predefined queries to identify the subject, the predefined queries defined in advance by agreement with respective owners of each of the multiple independently operated databases, and at least one of the predefined queries requiring at least one item of out-of-wallet data in an answer to the query; and

a verification engine for facilitating authentication of the subject by receiving the authentication request, selecting one or more of the predefined queries, including at least one of the predefined queries that requires at least one item of out-of-wallet data in an answer to the query, presenting the one or more selected queries to the subject via the authenticating client, receiving from the subject an answer to each of the one or more

[8] See claims 1, 13, 19, 21.

selected queries, and presenting the answer, including at least one item of out-of-wallet data, to each of the multiple independently operated databases for a validation response.

A. Shapiro Does Not Teach A Verification Engine For Facilitating Authentication Of The Subject By Presenting The One Or More Selected Queries To The Subject Via The Authentication Client

Claim 1 refers to "a verification engine for facilitating authentication of the subject by receiving the authentication request, selecting one or more of the predefined queries, presenting the one or more selected queries to the subject via the authenticating client, receiving from the subject an answer to each of the one or more selected queries, and presenting the answer to each of the multiple independently operated databases for a validation response" (quoting claim 1 with emphasis added).

Applicant does not see where Shapiro teaches "a verification engine for facilitating authentication of the subject ... by presenting the one or more selected queries to the subject via the authenticating client" (quoting claim 1 with emphasis added).[9] This was discussed above in the summary of Shapiro.

B. Shapiro does not disclose presenting predefined queries that require out-of-wallet data in the subject's answer

Claim 1 also calls for, "selecting one or more of the predefined queries, including at least one of the predefined queries that requires at least one item of out-of-wallet data in an answer to the query, presenting the one or more selected queries to the subject via the authenticating client, receiving from the subject an answer to each of the one or more selected queries, and presenting the answer, including at least one item of out-of-wallet data, to each of the multiple independently operated databases for a validation response."

Shapiro does not disclose presenting this type of query to the subject, nor does he suggest the use of such a query together with the subject's answer in seeking validation by a third party.

Having failed to identify each and every element of claim 1, the Office action has not established a prima facie case of anticipation. *Celeritas Techs. Inc. v. Rockwell Int'l Corp.*, 150 F.3d 1354, 1360 (Fed. Cir. 1998) (a rejection based on prior art must account for *each and every* claim limitation).

[9] See also discussion of claim 6 below.

IV. Shapiro does not provide a confidence level of the putative identity of a subject – Claims 4, 5, 17, 20 and 21

Claim 4 and its respective dependent claims are patentable over Shapiro for similar reasons. In addition, claim 4 refers to "a verification engine to receive from the authentication subject, via the authentication client, an answer to each of the predefined queries, to obtain from each of the plurality of independent database systems a corresponding authentication confidence for each answer, and to combine the corresponding authentication confidence for each answer into a combined authentication confidence." (quoting claim 4 with emphasis added). Applicant does not see where Shapiro teaches "a verification engine . . . to combine the corresponding authentication confidence for each answer into a combined authentication confidence." In fact, the word "confidence" does not even appear in Shapiro at all. For at least these reasons, the Office action does not provide evidence that Shapiro anticipates claim 4.

Claim 5 is currently amended only in the preamble to recite:

"A user ~~authorization~~ identity authentication method comprising the steps of:

presenting to an authentication subject one or more predefined queries, the predefined queries defined in advance by agreement with owners of each of multiple independent databases, the multiple independent databases storing identifying information about the authentication subject;

receiving from the authentication subject an answer to each of the selected queries;

presenting each answer to at least one of the multiple independent databases that has corresponding identifying information;

selecting at least one independent data source;

obtaining from the ~~multiple~~ independent ~~databases~~ data source an authentication confidence level for each answer; and

combining the authentication confidence level for each answer into a combined confidence level for authenticating the authentication subject."

Thus, in the method of claim 5, *predefined queries* are submitted *to the user* (authentication subject). This is contrary to operating on data first selected and input *by the user*. In this way, the user cannot predict or control what questions might be asked of him. The claim further calls for, "receiving from the authentication subject an answer to each of the selected queries." Importantly, these answers are *from the user*; not from a third-party. Next, the method calls for selecting at least one independent data source.

Again, this data source is selected by the system, not input by the user, so that fraud or malfeasance are avoided. Finally, an authentication confidence level is obtained, i.e., the data source provides an indication as to whether the answer given by the user is correct. For at least these reasons, claims 5 and 20 should be allowed.

Claim 21 recites, "The method of claim 5 wherein the identifying information [stored in the independent data sources] includes out-of-wallet data identifying the authentication subject." As noted above, Shapiro does not disclose this use of out-of-wallet data. For this additional reason, claim 21 should be allowed.

Claim 17 recites:

"17. (Previously presented) The system of claim 1 wherein the verification engine further facilitates authentication of the subject by:

receiving the validation responses from each of the multiple independently operated databases, the validation responses including a match confidence; and

determining an overall authentication confidence based on each of the received match confidences."

This analysis of match confidence is not disclosed in the reference cited by the examiner.[10] For this additional reason, claim 17 should be allowed.

V. The Process of Claim 6 is Not Anticipated

Against the foregoing backdrop, we review the limitations of claims 6 as currently amended.

"6. (Currently amended) A method of authenticating the putative identity of a subject who is an individual, the method comprising the steps of:

"negotiating a predetermined set of permitted types of queries with an owner of an independent, remote, third-party database, the independent, remote, third-party database including identifying information associated with the subject;

"providing a database interface for interacting with the independent, remote, third-party database without storing any significant portion of the third-party database locally, and wherein the interaction is limited to submitting a query among the predetermined set

[10] See specification at [0014].

of permitted types of queries, and receiving from the third-party database a response to the permitted query;

"responsive to a request from a client to authenticate the putative identity of a subject, forming a first query to elicit from the subject at least one item of information sufficient to form one of the permitted types of queries, and sending the first query to the subject via the client;

"receiving identifying information associated with the subject in response to the first query to authenticate his identity, the received identifying information including at least one item of information sufficient to form one of the permitted types of queries;

"forming a permitted type of query based on the received identifying information;

"transmitting the formed query to the remote, third-party database; and

"receiving a response from the remote, third-party database wherein the database interface does not otherwise provide access to the remote, third-party database, so that privacy of the remote, third-party database content remains under control of its owner."

The newly added limitation above calls for receiving a request from a client to authenticate a subject. In response to such a request, the method forms a first query, to elicit certain information, and sends the first query to the subject via the client. For example, where a customer (subject) is accessing an E-Commerce Site (client), the commerce site may interact with a verification engine which in turn sends the first query to (or for) the subject to provide identifying information. Shapiro does not disclose this scenario; it does not form any query to the subject. Rather, Shapiro merely forms a verification query to a third-party selected by the user, to verify data already selected, input and stored by the user.

Next, in claim 6 above, the method recites receiving the requested information from the subject (in response to the first query). By contrast, Shapiro does not disclose receiving a response from the subject; it only sends queries to a third-party.

Finally, in claim 6, the information received from the subject, in response to the first query, is used to form "a permitted type of query" i.e. one to which a third-party vendor has agreed to respond. That permitted type of query is "based on the received identifying information" from the subject.[11] But the questions may not known to the subject in advance.

---

[11] To illustrate, various [*question:answer*] pairs may be submitted to the third-party database proprietor ("Trusted Validator" (3a) for example).

Thus it may be seen that while Shapiro uses certain terms that are similar to those appearing in the present claims (similar enough perhaps to cause confusion), the structure and organization of that system is quite different, and it serves a different purpose. Anticipation of course requires that all limitations of the claim be disclosed in the reference, arranged in the same manner as the claim. That is not the case here. For at least the reasons shown above, the pending claims not anticipated and should be allowed.

VI. Claims 16 and 18 are Directed to E-Commerce

Claim 16 refers to "the system of claim 1 wherein the authentication client includes an electronic commerce site" (quoting claim 16). Applicant does not see where Shapiro discusses an electronic commerce site. In fact, "electronic commerce site" or "electronic commerce" do not even appear in Shapiro. For at least these reasons, the final Office action does not provide evidence that Shapiro anticipates claim 16. Accordingly, claim 16 is patentable over Shapiro. For similar reasons claim 18 is patentable over Shapiro.

Conclusion

In view of the foregoing, the Applicant submits that all claims are in condition for allowance. Therefore issuance of the Notice of Allowance is respectfully requested. The Examiner is welcome to call the undersigned to discuss any aspect of this application.

Respectfully submitted,

RAF Technology, Inc.

By: /MICAH D. STOLOWITZ/

Micah D. Stolowitz
Registration No. 32,758

STOLOWITZ FORD COWGER LLP
621 SW Morrison Street, Suite 600
Portland, OR 97205
(503) 224-2170